IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA

v.

HAILONG ZHU,

Defendant.

Case No. 1:23-cr-81

Count 1: 18 U.S.C. § 1956(h) (Conspiracy to Commit Money Laundering)

INDICTMENT

April 2023 Term — Alexandria

THE GRAND JURY CHARGES THAT:

At all times relevant to this Indictment:

GENERAL ALLEGATIONS

1. HAILONG ZHU ("ZHU") was a citizen of China and resided in multiple locations in the United States, including in Illinois and California.

2. Unindicted Co-Conspirator 1 ("Co-Conspirator 1") was a citizen of the United States and resided in California.

Business Entities

3. Sea Dragon Remodel Inc. was a company registered with the California Secretary of State on or about October 17, 2022. According to records, Sea Dragon Remodel was to be involved in "remodel [sic] and distribution of construction material." ZHU was the sole registered agent for this company as well as the Chief Executive Officer.

4. Sea Dragon Trading LLC was a company registered with the California Secretary of State on or about September 8, 2022. According to records, Sea Dragon Trading was to be engaged in "general trading." ZHU was the sole registered agent for this company as well as the Chief Executive Officer.

The Victims

5. Victim 1, an individual whose identity is known to the Grand Jury, was a resident of Falls Church, Virginia, within the Eastern District of Virginia during the time of the events discussed herein. Victim 1 transmitted funds to bank accounts associated with ZHU.

6. Victim 2, an individual whose identity is known to the Grand Jury, was a resident of New Jersey. Victim 2 transmitted funds to bank accounts associated with ZHU.

7. Victim 3, an individual whose identity is known to the Grand Jury, was a resident of California. Victim 3 transmitted funds to bank accounts associated with ZHU.

Terminology

8. "Digital currency" or "virtual currency" is currency that exists only in digital form; it has the characteristics of traditional money, but it does not have a physical equivalent. Cryptocurrency, a type of virtual currency, is a network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrency are Bitcoin (or BTC) and Ether (or ETH).

9. The term "spoofed" refers to domain spoofing and involves a cyberattack in which fraudsters and/or hackers seek to persuade individuals that a web address or email belongs to a legitimate and generally trusted company, when in fact it links the user to a false site controlled by a cybercriminal.

10. In so-called "pig butchering" schemes (a term derived from a foreign-language phrase used to describe these crimes), scammers encounter victims on dating services, social media websites, or even unsolicited texts or calls masquerading as a wrong number. Scammers initiate relationships with victims and slowly gain their trust, eventually introducing the idea of making a business investment using cryptocurrency. Victims are then directed to other members of the scheme running fraudulent cryptocurrency investment platforms and applications, where victims are persuaded to invest money. Once the money is sent — either through a fraudulent investment service or more traditional bank wires — the investment platform may show significant gains on the purported investment, and the victim is induced to invest or send additional money. Ultimately, the victim is unable to withdraw or recover their money, often resulting in significant losses for the victim.

COUNT 1

(Conspiracy to Commit Money Laundering)

11. The Grand Jury re-alleges and incorporates by reference paragraphs 1 through 10 of this Indictment.

12. From at least September 2022 and continuing through on or about March 21, 2023, more exact dates being unknown to the Grand Jury, in the Eastern District of Virginia and elsewhere, the defendant, HAILONG ZHU, did knowingly and intentionally combine, conspire, confederate, and agree with Co-Conspirator 1 and others, both known and unknown to the Grand Jury, to commit a violation of Title 18, United States Code, Section 1956, namely, to conduct and attempt to conduct a financial transaction which involved the proceeds of specified unlawful activity, that is, wire fraud, knowing that the transaction was designed in whole or in part to conceal and disguise the nature, location source, ownership, and control of the proceeds of specified unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(l)(B)(i).

PURPOSE AND OBJECT OF THE CONSPIRACY

13. The primary object of the conspiracy was for the conspirators to enrich themselves by fraudulently obtaining money and property from victims through electronic communications, and to conceal and obscure the source of the fraudulently obtained proceeds they received by transferring the proceeds between multiple bank accounts, and ultimately outside the United States.

WAYS, MANNERS, AND MEANS

14. The ways, manners, and means by which ZHU and his co-conspirators carried out the primary objects of the conspiracy included, but were not limited to, the following:

15. The conspirators met victims through unsolicited telephone calls online dating services.

16. The conspirators gained the trust of victims by establishing either professional or romantic relationships with the victims. These built these relationships by using a variety of means and facilities of interstate communications including, but not limited to, electronic messages sent via end-to-end encrypted applications.

17. The conspirators promoted "cryptocurrency investments" to the victims after gaining the victims' trust.

18. The conspirators established "spoofed" domains and websites that resembled legitimate cryptocurrency trading platforms.

19. The conspirators then fraudulently induced some victims into "investing" in cryptocurrency through these fraudulent and spoofed investment platforms.

20. The conspirators also fraudulently induced some victims into "investing" in cryptocurrency by sending funds via wire transfer.

21. The conspirators fraudulently represented to victims through the spoofed domains that the victims' "investments" were appreciating when, in fact, the victims could no longer access their monies or obtain their return.

22. ZHU and other conspirators based in the United States registered corporate entities with the California Secretary of State.

23. ZHU and other conspirators then opened bank accounts in the corporate entities' names with United States financial institutions.

24. ZHU and other conspirators' bank accounts received interstate wire transfers from victims.

25. ZHU and other conspirators arranged for the transfer of the fraudulently obtained proceeds via interstate and international wire transfers.

26. Co-Conspirator 1 directed ZHU and other conspirators on how to register corporate entities with the California Secretary of State.

27. Co-Conspirator 1 directed ZHU and other conspirators on how to open bank accounts with United States financial institutions.

28. Co-Conspirator 1 directed ZHU and other conspirators on when and how to execute interstate and international wire transfers.

29. Co-Conspirator 1 had online access to the bank accounts opened by ZHU and other conspirators. Co-Conspirator 1 used this online access to review the bank accounts, execute wire transfers, and communicate with United States financial institutions when the accounts were restricted by the financial institutions.

30. Co-Conspirator 1 placed voice calls to United States financial institutions and falsely represented that he was the accountholder when, in fact, ZHU or another conspirator was the accountholder. During these calls, Co-Conspirator 1 tried to obtain illegal proceeds that had been frozen.

31. ZHU, Co-Conspirator 1, and other conspirators communicated with each other and coordinated acts in furtherance of the conspiracy through MESSAGING SERVICE A.

32. ZHU, Co-Conspirator 1, and other conspirators received monetary compensation for their role in the conspiracy.

OVERT ACTS

33. In furtherance of the conspiracy and to effect the objects thereof, ZHU and his co-conspirators committed overt acts in the Eastern District of Virginia and elsewhere, including, but not limited to, the following:

Bank Accounts

34. On or about September 9, 2022, ZHU opened an account with account number ending 3886 with J.P. Morgan Chase in the name of Sea Dragon Trading LLC. ZHU was the sole signatory for this bank account.

35. On or about October 20, 2022, ZHU opened an account with account number ending 9529 with Bank of America in the name of Sea Dragon Remodel Inc. ZHU was the sole signatory on this account.

36. On or about October 21, 2022, ZHU opened an account with account number ending 5581 with J.P. Morgan Chase in the name of Sea Dragon Remodel Inc. ZHU was the sole signatory on this account.

Victim 1

37. In or around May or June 2022, Victim 1 received an unsolicited call from a woman identifying herself as "Rachel." Shortly after this call, Victim 1 and "Rachel" began communicating on Telegram, which offers end-to-end encrypted messaging. "Rachel" claimed to live in Miami, Florida.

38. "Rachel" led Victim 1 to believe that they were in a romantic relationship.

39. "Rachel" began discussing cryptocurrency investments with Victim 1. In particular, "Rachel" provided a link to a fraudulent cryptocurrency investment domain named "coinasx.com" where Victim 1 was led to download an application directly from "coinasx.com"

to his mobile device. The downloaded platform used the name "ASX," which mimicked the Australian Securities Exchange.

40. Victim 1 spoke with a purported customer service representative on the "coinasx.com" online chat portal, who explained to Victim 1 how to invest in "coinasx.com."

41. "Rachel" encouraged Victim 1 to invest in "ASX."

42. Victim 1 agreed to make his investments into "ASX" by sending wire transfers.

43. On or about August 12, 2022, within the Eastern District of Virginia, Victim 1 was fraudulently induced to send a wire transfer of $1,100 to an Evolve Bank & Trust account with account number ending in 2547.

44. On or about September 15, 2022, within the Eastern District of Virginia, Victim 1 was fraudulently induced to send a wire transfer of $3,100 to a Community Federal Savings Bank account with account number ending in 9471.

45. On or about September 30, 2022, within the Eastern District of Virginia, Victim 1 was fraudulently induced to send a wire transfer of $15,100 to an Evolve Bank & Trust account with account number ending in 7199.

46. On or about October 18, 2022, within the Eastern District of Virginia, Victim 1 was fraudulently induced to send a wire transfer of $2,420 to a Choice Financial Group account with account number ending in 6584.

47. On or about November 17, 2022, within the Eastern District of Virginia, Victim 1 was fraudulently induced to send a wire transfer of $5,000 to an Evolve Bank & Trust account with account number ending in 7248.

48. On or about November 25, 2022, within the Eastern District of Virginia, Victim 1 was fraudulently induced to send a wire transfer of $5,000, which originated in the Eastern

District of Virginia and transited through Pennsylvania, from his Bank of America account to ZHU's Sea Dragon Remodel Inc. account with account number ending 9529.

49. On or about November 25, 2022, ZHU withdrew $20,000 in cash from the Bank of America account with account number ending 9529. On or about November 29, 2022, $53,000 was wired to an account at Mitsubishi UFJ Trust and Banking with instructions that it be further wired on to at least one other account.

Victim 2

50. On or about September 2, 2022, Victim 2 received an unsolicited call from an individual identifying herself as "Eileen," who represented she was from the Los Angeles area. "Eileen" asked if Victim 2 was interested in speaking about cryptocurrency investments, and "Eileen" and Victim 2 then began communicating about cryptocurrency investments on Telegram. Victim 2 believed he had a friendship with "Eileen."

51. In September 2022, "Eileen" provided Victim 2 a link to a fraudulent cryptocurrency investment domain named "bitkancoin.com" where Victim 2 download an application directly from "bitkancoin.com" to his mobile device to create an account and begin making "investments." "Eileen" provided Victim 2 with wire instructions to make "investments."

52. On or about September 21, 2022, Victim 2 was fraudulently induced to send a wire transfer of $3,000 to a Choice Financial Group bank account with account number ending in 6584.

53. On or about November 2, 2022, Victim 2 was fraudulently induced to send a wire transfer of $20,000 to ZHU's Sea Dragon Remodel Inc. J.P. Morgan Chase account with account number ending 5581.

54. On or about November 3, 2022, an online wire transfer for $50,000 was initiated from J.P. Morgan Chase account with account number ending 5581 to an account at Mitsubishi UFJ Trust and Banking bank with additional wire instructions directing that the money ultimately be transmitted to an overseas bank account with Deltec Bank.

Victim 3

55. On or about August 24, 2022, Victim 3 met an individual identifying himself as "Daniel" on an online dating service. Shortly after meeting, Victim 3 and "Daniel" began communicating on encrypted messaging services Telegram and WhatsApp. From in or around August 2022 to in or around October 2022, "Daniel" led Victim 3 to believe that they were in a romantic relationship.

56. In or around August 2022, "Daniel" began promoting cryptocurrency "investments" through the domain m.gammaex.net. "Daniel" instructed Victim 3 to consult the online customer service portal to begin making "investments."

57. From in or around August 2022 to in or around October 2022, Victim 3 was fraudulently induced to send approximately $84,000 in funds through wire transfers.

58. In or around September 26, 2022, Victim 3 was fraudulently induced to send a wire transfer of $25,000 to an Evolve Bank and Trust account with account number ending in 4931.

59. On or about October 12, 2022, Victim 3 was fraudulently induced to send a wire transfer of $31,000 to ZHU's Sea Dragon Trading LLC account with J.P. Morgan Chase with account number ending in 3886.

60. On or about October 17, 2022, ZHU wired $40,000 from his account with account number ending in 3886 to an account at Mitsubishi UFJ Trust and Banking with additional wire

instructions directing that the money ultimately be transmitted to an overseas bank account with Deltec Bank.

61. On or about October 24, 2022, Victim 3 was fraudulently induced to send a wire transfer of approximately $28,000 to a Cathay Bank account with account number ending in 0810.

(All in violation of Title 18, United States Code, Section 1956(h).)

FORFEITURE NOTICE

THE GRAND JURY FINDS PROBABLE CAUSE FOR FORFEITURE AS DESCRIBED BELOW:

Pursuant to Rule 32.2(a), the defendant is hereby notified that, if convicted of the money laundering offense alleged in Count 1 above, he shall forfeit to the United States, pursuant to 18 U.S.C. § 982(a)(1), any property, real or personal, involved in the money laundering offense of conviction, or any property traceable to such property.

If any property subject to forfeiture is unavailable, the United States may seek an order forfeiting substitute assets pursuant to Title 21, U.S. Code, Section 853(p) and Federal Rule of Criminal Procedure 32.2(e).

The property subject to forfeiture includes, but is not limited to, a sum of money equal to at least $56,000 in United States currency, representing the amount of money involved in the violation of 18 U.S.C. § 1956(h).

(In accordance with Title 18, United States Code, Section 982(a)(1) and Rule 32.2(a), Federal Rules of Criminal Procedure.)

A TRUE BILL

Pursuant to the E-Government Act, the original of this page has been filed under seal in the Clerk's Office.

Foreperson of the Grand Jury

Jessica D. Aber
United States Attorney

By: _____
Zoe Bedell
Carina A. Cuellar
Assistant United States Attorneys

By: _____
Georgiana L. MacDonald
Assistant United States Attorney
National Cryptocurrency Enforcement Team
Department of Justice